Digital Humanitarian Archives Toolkit

About this toolkit

Why are archives important for humanitarians?

Introducing digital archives

Key concepts

Section 1: Advocacy

Section 2: Deciding what to keep

Section 3: Choosing archive storage

Section 4: Moving records to the archive

Section 5: Preserving the archive long term

Section 6: Further steps

List of resources

Other useful toolkits and training

MANCHESTER 1824
The University of Manchester
John Rylands Research Institute and Library

DHM
Developing Humanitarian Medicine
A HISTORY OF NORMS, KNOWLEDGE PRODUCTION AND CARE

About this toolkit

Who is this toolkit for?

This toolkit is aimed at people working in a variety of roles (from executive to operations) at organisations who carry out humanitarian work who are interested in establishing an archive. No archiving knowledge or experience is needed to use it.

What is the aim of this toolkit?

This toolkit aims to help humanitarian organisations produce sustainable and useful digital archives from the records that they create over the course of their work. This includes records created in fieldwork as well as those created in a more formal office setting.

This toolkit doesn't give a single 'ideal' solution but explains the factors that should be considered to build your own solution.

How to use this toolkit

The toolkit is divided into stages, which can be followed from section 1 onwards. Each section ends with a link to an outcome form to be downloaded and completed before moving onto the next section. These forms are meant to help you structure and track your progress, but they can also be used as the basis for policies and processes for managing your digital archives.

The process outlined doesn't have to be strictly followed in order– decisions made in earlier sections can be changed at a later stage, and the process can be repeated if necessary. If you already meet the requirements for a particular section (as outlined in the outcome form) before you have started this process, you can start at the next section.

Reading through this toolkit fully before starting is also recommended. Sometimes, a later part of the process might affect a decision made earlier on.

At the end of this toolkit is a list of resources relevant to each section. If you'd like to know more about anything mentioned in that section, these links will provide some useful information.

How this toolkit was created and where it has been shared

This toolkit was written with reference to existing guides, research, toolkits and policies, in particular guidance created by the Digital Preservation Coalition (DPC) and the UK National Archives. See the 'Other useful toolkits' section for other related and useful guides, some of which were referred to in the creation of this toolkit. It was also created in consultation with humanitarian organisations (including Médecins Sans Frontières and the Mines Advisory Group) and the University of Manchester Library Special Collections department.

Why are archives important for humanitarians?

In every field of work, archives are important as first-hand evidence of events, opinions, discussions, decisions and activities that happened in the past. Unlike other sources, such as written histories, they allow us to reconstruct and reinterpret the past repeatedly, to look for something different. When archives don't survive, we lose the ability to do this.

Humanitarian work has an enormous impact on the lives of people, particularly those in vulnerable situations. They operate in complex conflict, post-conflict and natural disaster contexts, many of which are linked to historically and politically important events. Their archives are therefore very important sources.

Importance of archives to day-to-day humanitarian operations

Archives can allow an organisation to reflect on past mistakes, successes, processes and decisions to inform their current and future work, which helps them continuously improve and avoid repeating mistakes.

For humanitarians, this means they are not starting from scratch each time they begin a new operation or mission, but instead working from a solid basis of knowledge taken from previous experience.

It can also make working more efficient: being able to easily find out what records you have, and where they are, saves time and reduces the number of records that are duplicated.

It gives an organisation more control over their documentation, as they are aware of what is being kept and what isn't (for this reason, it can sometimes even help to free up storage space).It also helps to preserve institutional knowledge in a sector which works in dispersed, emergency settings which experiences a high turnover of staff.

An archive can also act as a strong evidence base which can help with legal requirements and providing accountability information to funders.

Importance of archives to humanitarian organisations

An archive represents an organisation's institutional memory: through it, people working there can learn about its history and guiding principles to inform their day-to-day work and to feel more connected to the collective purpose.

If a humanitarian organisation invests in maintaining its archive, it demonstrates transparency, responsibility and accountability, a willingness to learn from past mistakes and to take ownership of how the organisation has affected the lives of the communities they have worked with. Keeping records also shows responsibility towards these communities, who have a right to have their experience accurately recorded and securely kept in the archive.

Some would argue that keeping records of wrongdoing, even if they are closed, risks damaging the reputation of the organisation if they are leaked. However, evidence of an organisation destroying such archives as a cover up is arguably more damaging. Working with transparency demonstrates a commitment to being accountable to stakeholders, the public, and the populations that humanitarians work to help.

Importance of humanitarian archives to history

Humanitarians have been present for some of the most important historical events of the past century. They have come closer than most people to the wars, disease outbreaks and disasters which have shaped the world, as witnesses to the way in which events and political decisions coalesce to affect people's lives.

The preservation of this in archives allows others looking back on these events to take this unique and crucial perspective into account, and as history is being made today its preservation must be considered now.

Ever since the shift to digital working, humanitarian archives are more at risk of being lost, due to the complexities of preserving digital records. It is now more important than ever to make sure that this work is recorded and preserved for the future.

Introducing digital archives

Archives

An archive is made up of records created or used by a person or organisation during their work, which act as evidence of this work. They can contain useful information, and they also act as evidence of decisions, tasks, discussions and activities happened. They are unique, naturally created (i.e. not written with the intention of being historical evidence) and can be kept by the organisation or person that created them or deposited with a library or archives centre.

Archives are often managed by an archivist. Archivists are trained in processes and principles which help them to catalogue, manage the long-term preservation of, and control access to archives. Many organisations with archives do not have an archivist, and it is possible to manage an archive without one.

Digital archives

Archives can be in almost any format, including digital. As a lot of work is now carried out electronically, many records created today that will become archives are in a digital format, including as spreadsheets, databases, emails, documents, and digital images.

These digital archives come with new difficulties which paper archives don't have. Digital files can become corrupted, and the file formats, software and hardware used to create and access these files change rapidly over time. This can mean that older files quickly become difficult, or impossible, to access.

Digital preservation

Digital files therefore need a more 'active' management and consistent monitoring over time, to make sure that any actions needed to keep them accessible, like transferring a record from an obsolete file format to a newer one, happen promptly.

The work of keeping digital material secure, readable and accessible over the long term is called digital preservation. Digital preservation involves technical solutions but also principles and processes to ensure that material is preserved.

Key concepts and glossary

To get started working with digital archives, there are a few technical concepts that are key to understand, as they will come up throughout this toolkit. To find out more about each of these concepts, see the relevant section of the resources page.

Appraisal

Appraisal is the practice of assessing which records do or don't have long term historic value, and so what should go into an archive

Archives

Archives are collections of records created by people or organisations which provide evidence of actions, decisions and discussion. They can come in lots of different formats, including in digital formats.

Bit rot

At their very base, digital files are made up of binary digits, or 'bits', which are a series of 1s and 0s that a computer reads and translates into a human readable form (such as a photo, or a written document). Over time, these bits can 'flip', turning from a 1 to a 0 or vice versa. This process, also called 'bit rot', makes a file corrupted and unreadable.

Checksums

The integrity of a file can be monitored using checksums. A checksum is a long, unique string of numbers and letters which can be created for a file, or a group of files, using a variety of different tools. If anything in the file has changed, then the checksum made after this change will not be the same as the one before. Creating checksums is an easier way of checking whether a group of files have been altered or corrupted without having to look through each one. To get started working with digital archives, there are a few technical concepts that are key to understand, as they will come up a lot throughout this toolkit.

Digital preservation

Digital preservation refers to the actions and processes which are carried out to keep digital files accessible over time, tackling technological obsolescence and file corruption.

Metadata

Metadata literally means 'data about data'. For digital archives it refers to the information about the digital files such as their creator, dates of creation and modification and access permissions. Metadata is very important for proving a file's identity and authenticity, and for tracing the changes that it has been through. Metadata can be embedded and automatically generated as part of a file's properties, but it also includes information that is created about the content – e.g. a database that records changes made to a file, or a description of a group of files.

Technology obsolescence and proliferation

The file formats, software, and hardware that we use to create electronic records are changing all the time. New ways of creating and accessing files are constantly appearing, while old ones fall out of use. This causes difficulties in accessing old digital files which are no longer supported, and in trying to find solutions for preserving lots of new kinds of files.

Section 1: Advocacy

Creating and maintaining a digital archive is a task which requires resources: money, people's time, and altering the ways people work. This can be a big change to the way your organisation works, and so the first step is to get support for the idea, particularly from key stakeholders.

What to say

To help you talk to people about archives, it can help to have some key points written down that you can present to people or use as discussion points.

You could adapt some of the suggestions in the "*Why are archives important for humanitarians?*" section to introduce people to the topic and to demonstrate the benefits of having an archive.

If you can, link it to specific examples, facts and figures from your organisation and the work that you do, and any strategic plans or mission statements that you have.

The first part of the outcome form for this section contains space for you to note these down.

How to talk to people

Discussions about archiving can start in a number of ways. You could start by talking to the people around you informally about it, to see if they are interested. You could also bring it up in department meetings, or any other discussion spaces at your organisation, to bring it to people's attention.

When you are advocating, it is better to do this alongside other people, to show that there is wider support in the organisation. If you find other people are also interested in the issue, then encourage them to support you.

Tips

When talking to people about digital archives, remember to:

- Tailor your arguments to your audience and the issues that matter most to them in their work: this could be budgets, IT, information security, legal issues or organisational strategies.
- Listen to people: take time to address their concerns and take their suggestions on board.
- Be honest and realistic too: creating a digital archive will involve people's time and money, so instead of minimising this, demonstrate the benefits it will provide.

Who to talk to

There are some roles within an organisation whose support you will need to implement digital archiving, and who you will need to make the case to in order to be able to put this into practice.

These might not be specific roles within your organisation, but may be included alongside other responsibilities for staff members or departments. There also might not be someone responsible for these things, particularly if you work in a small organisation, but you should check before assuming that there isn't.

- Senior members in the organisation: given the resources that are required for archiving, it is important to have support from someone senior in the organisation who can approve this.
- Information Technology (IT): digital archiving is a technical process, and you will need input and support from someone in your organisation who maintains your digital infrastructure.
- Data protection, records management, information governance, paper archives: anyone who has responsibility for managing information, data and records, or any paper archives you might have, should also be involved. They will be able to inform on existing practices and any relevant regulations.

You don't need everyone in your organisation who has these responsibilities to be involved, but at least one person from each, to ensure representation. These people, along with anyone else who is interested in the project, will form your key stakeholders group. This group will discuss and sign off on each stage of planning for the process (there is a section for this at the end of each outcome form). The second part of the outcome form includes space for you to note down these names.

You should have a specific and realistic goal, that your key stakeholders can agree to support. This could include an agreement to carry out the process outlined in this toolkit with their support, and for someone, or a group of people at your organisation, to be able to commit some of their time to it. The third section of the outcome form includes space for you to write this down.

Continuing advocacy

Advocacy is a continuous process. Even with key stakeholders on board, you will need to keep making the case for a digital archive as the project grows and more people become aware of it, particularly if you run into difficulties. Digital archiving requires everyone in an organisation to contribute in some way, and many people may be reluctant to do this on top of heavy workloads and time pressure.

You may want to consider formulating a communications strategy to underpin the high-level organisational benefits of maintaining an archive, highlighting its alignment with overall organisational commitments to good governance, digital innovation, and effective ways of working.

You could also explore creating a partnership with a higher education institution or charitable institution looking for hands-on experience in archiving as one way to resource the work needed, alongside tasks undertaken by staff members.

Section 1 outcomes

It would benefit our organisation to keep and look after our archives because:

You can use arguments from the 'Why are archives important for humanitarians' section. Include facts, figures, operational and strategic plans and evidence from your own organisation if you can find them.

The key stakeholders (KS) we will engage with this plan are (add names and roles):

Management:

Information Technology:

Data protection, records management, information governance, paper archives:

Other interested parties:

Our initial plan is to:

e.g. trial an archive process in one department, carry out the process outlined in this toolkit

Approval of KS for the above:

Names, roles and date agreed

Section 2: Deciding what to keep

Once you have the backing needed to implement digital archiving, the next step is to work out which records to keep permanently. This is something you will need to decide initially at a higher level; in terms of what types of information you want to preserve. Then, you will need to decide how this applies to each department's records.

What do you need to keep?

The first thing to consider is whether there are any records whose retention or disposal is subject to regulation, which means that you need to keep them for a certain amount of time and then dispose of them.

This often applies to:
- Medical records
- Records about your staff (i.e. HR records)
- Financial records

You should check what the regulations are around keeping these records in each country that you work in, and where you are headquartered, as regulations vary from country to country. If there is someone in your organisation responsible for information management, they should be able to help you with this. This will inform the retention period of the records, i.e. how long you keep them for.

It is a good idea to have an organisation wide policy about records retention, which follows the regulation for the country where headquarters are based. For work that covers multiple countries using the organisation wide policy should be used unless the national standards for one of the other countries are stricter, and then these regulations should be followed.

Depending on where your headquarters are located, you may need a policy on the protection of personal data. For example, if you are based in Europe you will need to comply with the General Data Protection Regulations (GDPR). These types of regulation require you to have a policy on how you handle personal data, which can affect how you archive it.

In cases of uncertainty, you could contact the governmental body responsible for charities for the country your headquarters is based in. For example, if you are based in the UK, the UK Charity Commission will be able to advise. It could also affect how you archive this information, as countries have different legislation on the movement of personal information across borders.

The outcome form for this section includes a table that you can use to outline the regulation that affects your records, if you want something to track this information with.

You should also consider if there are any records that you need to keep for other accountability purposes, for example if you receive funding from a certain body that requires proof of how the funding was spent to be kept.

There might be cases where you need to keep documents for many years before disposing of them, and which will need to be accessible for a long time. This means many of the preservation considerations you have for documents you keep permanently will apply to these also, and you might want to keep them in an archive space until you need to dispose of them.

What do you want to keep?

Once you have worked out what you need to do with your records, you can move on to working out what you want to keep for your archive.

You can do this through an archival process known as appraisal. Appraisal is the practice of assessing which records do or don't have long term historic value, and so what should go into an archive. It isn't possible (or a good idea) to keep every single document you create, so appraisal is a very important step to decide what will be preserved.

You may want to keep records that are evidence of:
- How your organisation operated:
  - Policies, processes, procedures
  - Agreements (memoranda of understanding, service level agreements) with key partners (including governments and donors)
- Discussions and debates about your work:
  - Meeting minutes, emails, notes of important conversations
- The impact of your work:
  - Data gathered on aid provided/the effect it had
  - Photographic/video evidence of your work.
- Successes, failures, and issues encountered during your work:
  - Reports, either internally or externally published
- How your work is publicised and communicated to different audiences:
  - Internal communications – newsletters, internal updates, situation reports
  - External communications – newspaper and journal articles, press and conference statements

You might want to discard records that are:
- Personal:
  - Messages about personal or social matters
  - Employees' personal information kept on work computers (e.g. employees' own copies of their payslips)
- Evidence of general administration activities, which doesn't demonstrate anything specific about your organisation:
  - Expense claims
  - Documentation of IT problems and solutions

Before you move on to applying these decisions practically, it is a good idea to write down a broad outline of the types of documents you will keep, possibly adapting some of the points above. This will give you something to refer back to when carrying out the next step. See the outcome form at the end of this section for a template for this.

Tips

- How much storage space you can afford to maintain long term is also important to consider at this stage, as this will affect whether you can afford to keep a broader or narrower range of your records.
- You should also consider the sizes of different file types: for example, image and video files generally take up a lot more storage space than documents.

Assessing communications

You could also consider including communications like emails, and any instant messaging you use, like WhatsApp, Microsoft Teams or Telegram, in your appraisal as these can also contain important information to archive. Again, it isn't practical to appraise this material by looking at each message, but as they aren't kept in structured folders this assessment is different. Emails are linked to individual accounts, while instant messages are linked to individuals and also groups of people, as they are often used to communicate between several different people in group chats.

One useful method for choosing which emails and messages to preserve is to pick out the roles and groups where the most important discussions are being had, to work out which email accounts and instant messaging groups should be archived. Remember that if someone in one of these roles or groups is expected to have their emails or messages archived, it is important to make this clear to them before this happens. This is particularly important for instant messages, which are often sent and stored from personal devices.

Similarly, if your organisation is active on social media, or if you have a website, you might also want to preserve this, as evidence of how your organisation's work was communicated to the public.

Preserving emails, instant messages and social media also involves more technical steps for storing, preserving and accessing them than ordinary digital files (for example they will need to be exported out of their clients and apps to be preserved) which you should consider before deciding to include them.

Applying appraisal

When it comes to applying these parameters to the records that your organisation creates, it is a good idea to see how they apply to each section or department of your organisation. This will involve assessing each department's records against the outline that you have agreed on above, and listing what records from that department or section will be archived.

You should also consider what important records are kept outside of your regular filing system, in e.g. line of business systems or case management systems, that you want to preserve, and how easy these are to extract from these systems for archiving.

The final section of the outcome form includes a table that you can fill out to record which sets of records will be archived from each department.

Tips

- Appraisal isn't a practical thing to do for each individual document you create. Instead, you should aim to do this at a folder level. Depending on how much time and resourcing you have to complete this step, you can carry it out at a different level of detail, i.e., at a higher or lower level of your filing systems.
- Thinking about how this appraisal will work may affect how you set up your filing systems in the first place, to make it easier to identify what records will be kept permanently, for a set period, and what will be disposed of.

Section 2 outcomes

These are the regulatory requirements that we need to adhere to:

For each, list the country it applies to, and the type of record – e.g. personal data, medical records, financial records. If there is anyone in your organisation responsible for information governance or similar, talk to them about this. You can fill out the table below to help record this:

Country applicable (e.g. UK)	Law/regulatory requirement (e.g. Data Protection Act 2018)	Records affected (e.g. medical records, personnel records)

We will permanently keep records that are evidence of (tick all that apply and add more at the end if required):

How our organisation operated
- *Policies, processes, procedures*
- *Agreements (memoranda of understanding, service level agreements) with key partners (including governments and donors)*
- *Discussions and debates about our work*
- *Meeting minutes, emails, notes of important conversations*

The impact of our work
- *Data gathered on aid provided/the effect it had*
- *Photographic/video evidence of your work.*

Successes, failures, and issues encountered during our work
- *Reports, either internally or externally published*

How our work is publicised and communicated to different audiences
- *Internal communications – newsletters, internal updates, situation reports*
- *External communications – newspaper and journal articles, press and conference statements*

We will dispose of the following records once they are no longer in active use (tick all which apply and add more at the end if required):

Personal records:
- *Messages about personal or social matters*
- *Employees' personal information kept on work computers (e.g. employees' own copies of their payslips)*

Evidence of general administration activities, which doesn't demonstrate anything specific about our organisation:
- *Expense claims*
- *Documentation of IT problems and solutions*

This is how this will apply to each section/department of the organisation:

To be filled out by the head(s)/leader(s) of each department, in consultation with you and your key stakeholders. If you can, add in specific names of folders that people regularly use, so it is easy to follow

Folders/document groups we will archive permanently (e.g. situation reports)	Folders/document groups we will keep for a set amount of time before disposing of them (state retention period: e.g. medical records, 70 years)	Folders/document groups we will dispose of once they are no longer in use (e.g. expense receipts)	Communications we will archive permanently (if applicable: e.g. full team WhatsApp chat, head of mission email account)

Approval of KS for the above:

Names, roles and date agreed

Section 3: Choosing archive storage

Once you have decided what you want to archive it's important to consider what kind of storage you will use for it. There are a few different options and not one perfect solution that works for everyone. Your decision will depend on your budget, the size of your archive (and how much you expect it to grow over time), and how accessible you want it to be.

Below are some important factors to consider when choosing a storage solution that is appropriate for long term digital preservation.

Sustainability

This archive storage needs to be sustainable, as this is a long term process that aims to keep these records permanently. Although no one storage system will last forever, you should consider that the solution you choose will need to be affordable and manageable over the long term: think realistically about how much money it will cost, and how much staff time is needed to maintain it.

Duplication

It is very important that, if something happens to one copy of your archives and they becomes inaccessible or are destroyed, that they can be duplicated from an additional copy. This is why it is recommended to have at least one other copy of your digital archives on a different storage system (e.g. by having one copy on a cloud storage area, and one on a hard drive) so that if anything happens to the files on one system, you can duplicate them from the other. Storing duplicate copies of files across different storage media does add an additional cost which should be considered.

Some cloud and most digital preservation systems provide this duplication as part of their service, although cloud providers may refer to it as 'data resiliency'. You should research any provider's approach to this before choosing to use their product and still think carefully about relying on just one storage solution.

Security and access

It is important that your storage solution allows you to ensure files cannot be edited, deleted, or moved and that access to the archive is controlled. Your archive may also contain sensitive data: you will need to be able to restrict access to this appropriately. You should also consider how people will access the digital archive once it is set up: will everyone have access to the archives storage, or will this be restricted to a few people who will 'retrieve' digital files for people who request them? How this works will affect what kind of storage you choose, and how accessible it is to people in your organisation.

Metadata preservation

Often, when files are moved to a different storage system, they lose their metadata – this is a particular problem with cloud storage. This is because the system they are being moved onto views these files as new and their date of creation becomes the date of upload and the creator becomes the person who uploaded it. This erases important information about the file, including when the file was created and who created it.

Before choosing a system, make sure that there is a way of migrating your files onto it which retains their important metadata, or, if this isn't possible, if there is a way of exporting the original metadata (e.g. into an excel spreadsheet) so it can be stored alongside the files in the archive.

Some cloud storage providers offer their own migration tool (like the SharePoint Migration Tool) which can help to prevent some of this. You should be cautious about third party migration tools which offer these services, as they can be expensive and may not deliver what they promise.

Permanence

Some storage systems, particularly cloud storage, are designed more for collaborative working than long term storage. This means that they may have features that don't make it suitable for an archive – for example automatic deletion policies. It is important to make sure that any system you choose doesn't have these features, or that they can be disabled.

Exit strategy

No storage solution will last forever, and so it is important that when the time comes to move your archive you can do so without it significantly affecting the integrity of the files or losing important metadata.

Different options for storage

Your decision on what archive storage you will use should involve your stakeholders, in particular anyone who is responsible for IT infrastructure, as they will need to support and maintain the system.

Your choice of archive storage may also be affected by the storage that you use for current documents. It can be easier to have your archive space and current document storage in the same type of storage but remember to think about how well it meets the requirements outlined above. If it doesn't, even if it is an easier solution now it could create issues in the future.

There are many options for storing digital archives but below are three popular solutions.

On site server storage

This is where your organisation manages and controls your file storage and computer systems using servers which are kept at the premises of the organisation, or in a location that they access. This solution gives you a lot of control over your digital infrastructure but it is also more resource intensive, as managing servers requires a lot of time from specialised staff.

If you do choose this solution, you should keep a backup copy on a different storage type, so that if anything happens to your servers, you still have a copy of your archive elsewhere.

If your current, day-to-day digital files are on a system like this it could be fairly straightforward to set up a section for archives on there. However, if you don't, this is a very costly method to set up from scratch.

Cloud storage

This is where an organisation pays a subscription to a third party to store their files on servers in data centres that the external company maintains. Examples include Google Drive, Amazon Web Services (AWS) and Microsoft SharePoint/OneDrive. Cloud storage requires less technical IT knowledge to manage it, as the servers used for storage are maintained by the company that owns them, and their user interfaces are generally user friendly. Cloud storage is also 'elastic', which means that when you need additional storage space, you simply pay a higher subscription fee instead of having to rebuild or change your storage system. Some cloud providers offer 'cold' storage, which is cheaper to buy as it isn't as easily accessible.

However, using cloud storage gives you less control over your files: you don't have control over the location of the server, or how the integrity of the files is managed, and if the company controlling these things stops operating this could harm your files or lead them to be lost.

Cloud storage is also often unreliable for some of the reasons outlined in the previous section: they overwrite the metadata of files uploaded to them and automatically delete certain 'temporary' files. Before setting up an archive on a cloud system, you should check for these issues, and if they are present that they can be reasonably worked around (e.g. by switching off automatic deletion features or using a built-in migration tool to move files with their metadata).

Third party specialist digital preservation storage.

There are also a number of third-party storage solutions which are specifically designed for digital preservation. These services can be expensive and still require input from your organisation to set them up and manage moving archives to the system. However, because they are tailored to digital preservation, they support the technical aspects of digital preservation like checking file formats and fixity, and duplicating files across different locations. Two popular examples include Preservica and Archivematica, although there are other solutions available.

Some document management systems will claim to offer preservation capabilities, but may not. Remember to research each potential new supplier carefully prior to committing to using them.

Section 3 outcomes

Our archives will be stored on (check all that apply – ideally two):

☐ *On site network server storage at our premises in on a drive/folder called*

☐ *cloud storage, in the area/folder called*

☐ *External hard drives, labelled stored securely in*

☐ *a digital preservation specialist provider*

We can confirm that, with our chosen archive storage, we can (add supporting information for each):

☐ *Sustain it long term, in terms of expense and staff time required to maintain it.*

☐ *Restrict editing rights and access in the archive to ensure that items in the archive are not modified post access, and sensitive information is kept restricted.*

☐ *Preserve the original file metadata once it has been moved to the storage area.*

☐ *Disable all auto deletion features that may be included in this storage area (if applicable)*

☐ *Get our files off this system and onto a new archive storage system with the filing structure and metadata intact.*

Approval of KS for the above:

Names, roles and date agreed

Section 4: Moving records to the archive

When to archive

Once you have decided what you want to move to an archive, and you have a storage space set up, you need to decide at what point your records should be added to the archive. You don't want to archive them too early (for example, if they are still being used, edited and added to) or too late - this can lead to them being left unmonitored for too long, and could risk them being lost.

It is a good idea to move records to an archive in groups, rather than individually. Moving records individually is more work and risks losing the context for them (like where they were stored in a filing structure) which can make their meaning more difficult to work out.

Some points that may trigger a group of documents being archived are:

- The end of a particular project or mission. If you have any activities that you already perform to 'close out' a mission or project then you can consider incorporating archiving activities into these.
- At a set time. For example, if you have a series of records which you create a new set of annually, you could archive them at the end of each year, once you have moved on to using a new set. It can be helpful to set aside a particular time each year to archive records, to help your organisation remember and make time for this.

Whatever decision you make, it's important to remember that records should not be changed once they are archived, so they need to be out of active use.

Preparing to archive

Once you've reached the point of archiving, there are some important things to have checked off before you consider transferring your records:

1. Tidying up the filing – making sure everything is in the right place, appropriately named, and anything which isn't going to be kept has been disposed of.
2. Extracting files that you want to preserve but which aren't kept on the main filing system – for example, if you have a particular instant messaging group, email or social media account that you want to preserve, then you will need to work out how to extract these files from their systems so that they can be stored with the rest of the archive. The same applies for any files kept on software that isn't your main storage system (e.g. databases).
3. Metadata – do the files have all their original, and necessary, metadata? This should include the date it was created and the creator and its security level/access permissions as a minimum. If you use additional metadata to organise and 'tag' your information you should consider preserving this too. This can include things like document type tags or the version of the document. See the outcome form at the end of this section for a list of essential and optional metadata.
4. Contextual information – there may be some information about the files, and the work that produced it, which isn't part of the files' metadata, for example, the roles of key document creators, or some background to what the project did, and explanations of any jargon. If you want to provide this, you could write it up in a short document which is preserved alongside the files.

Transfer

Whatever method you choose there are two key things that you need to consider when planning to move archives.

File and metadata integrity

Whatever method you use, you should ensure that the integrity of the files, and of their metadata, is preserved in the move to the archive. Moving files poses a risk to their integrity, as files can become corrupted and/or lost during moves. This should therefore be checked before and after they are moved This can be done using checksums – see the note on checksums in the 'Key concepts' section for more information on how these work.

Security

When moving archives, particularly sensitive archives, it is important to ensure that the method of moving them is secure and doesn't pose a risk to the information in the archives. This isn't something you need to consider if you are moving files within the same storage system, but if you are using any external tools you should check the security features of these.

Options for transferring archives

These include:

- Moving files: a 'drag and drop' might be possible if your archive is on the same system as your file storage, although this method poses a fairly high risk of files not being copied over properly, or being corrupted. A trusted file copying tool like Teracopy can help you identify if there are any errors in the files being copied and check the integrity of the files at each end of the process.
- Migration tools: some storage systems offer in-built migration tools which allow you to move files into the system while retaining metadata. This could be a good option if your archive location is different to your usual file storage.
- Compression tools: if your archive is very large it can be a good idea to compress it into a .zip file to move it. Note: compression methods are either lossy or lossless – lossy means that once the file is uncompressed, not all of the original file data is retained, whereas lossless compression means that all of the original data is retained.

There are also some methods that you should try to avoid:

- Email – sending your documents via email attachment is not a good method, as email attachments are not set up for sending large quantities of material, or folders.
- Portable storage – using portable storage, such as USB drives, to transfer archives, is also best avoided, as these objects can be easily lost, and may introduce viruses.

Embedding the process

As is often the case with work that happens on a temporary project basis, as humanitarian fieldwork mostly is, there is often not as much time and resources set aside to finish up a project as there is to set it up. This can leave the archives in limbo, as there is uncertainty about what to do with them, and as people leave an area of work the archives can easily be lost, damaged, or destroyed because no clear plan is made for them. This is why it is important to have a clear archiving process from to start, and to embed it into any other end of mission or mission closure activities that are in place.

Section 4 outcomes

We will move records that are selected for preservation to the archive once they are no longer in active use and (check all that apply):

☐ *At the end of the project/mission (the process is embedded into other end of mission activities)*

☐ *Every year, in:*

Before we send records to the archive, we will:

☐ *Ensure the filing is organised and folders and files have names which clearly indicate what they are*

☐ *Extract files that are due to be preserved but are not kept on our main filing system from the following systems (list here: e.g. WhatsApp, email, any line of business systems):*

☐ *Dispose of files which are not due to be preserved for any length of time.*

☐ *Marked up files which are due to be closed for a set amount of time, or destroyed at a certain point in the future.*

☐ *Ensure the files have the following metadata attached to them in some way:*

Element	Recorded at file or folder level
File name	File and folder level
File format	File level
File size	File and folder level
Security level	Folder level
Creator(s)	File and folder level
Date created	File and folder level
Date last modified	File and folder level
Review/disposal date (if applicable)	Folder level

Optional pre-archiving actions (check all that apply, if chosen):

☐ *Preparing a contextual 'front sheet' that outlines important contextual information about the mission/work, like the names and roles of key figures, background, definitions of any jargon used.*

☐ *Creating a checksum for the files (only necessary if a checksum will also be created after the files have been moved to check the file integrity post move)*

Our transfer method is (select one):

☐ *Drag and drop*

☐ *Using a trusted file copying tool, namely:*

☐ *Our storage system's in built migration tools, namely:*

After we have moved the files to the archive we will:

☐ *Check that none of the files have been lost/corrupted during the transfer by:*

☐ *Ensure that none of the files can be edited or moved from their filing structure by:*

☐ *Apply security measures to sensitive files by:*

The role/person responsible for preparing the archive to be moved is:

Add the name of the role which will be responsible for these tasks. Note: you can assign this job to multiple people, e.g. one role from each team.

Approval of KS for the above:

Names, roles and date agreed

Section 5: Preserving the archive long term

The goal of this process is to create a digital archive that can be understood, stored and accessed over the years by people who aren't necessarily familiar with the work that produced it.

The key to keeping digital archives is continuity. This involves consistent monitoring and carrying out any necessary preservation tasks as they come up as well as embedding the archive into the way your organisation works to ensure that it is valued and maintained in the future. These essential and optional (but strongly recommended) tasks are outlined in the outcome form for this section.

A good way to make sure the value of the archive is promoted throughout the organisation is to appoint archive representatives or 'champions'. These people can be from any area or department who have an interest in keeping the archive going. Their responsibilities will be to:

- Promote knowledge and use of the archive.
- Ensure that the archive is known about within the organisation, that it is considered when there are changes to the organisation or the way it works, and that the work on the archive is continued over the years.
- Respond to general or specific queries about the archive, accessing it and how it works.
- Advocating for improvements and resourcing for humanitarian digital archives and offering support to other organisations.

Section 5 outcomes

We have assigned the following responsibilities to ensure the preservation of the archive:

- [ ] *(Essential) Reviewing archiving processes and practices to ensure that they keep up with any changes to how you work: for example, if you move to using a different type of file storage, or if your organisation is restructured. This will be carried out by:*

- [ ] *(Essential) Reviewing archives that have a closure period or retention period, and potentially opening files that have been closed or destroying files whose retention period has expired. This will be carried out by:*

- [ ] *(Recommended) Monitoring the files for file integrity by:*

  This will be carried out by:

- [ ] *(Recommended) Monitoring the archive files for obsolescent file formats by:*

  This will be carried out by:

- [ ] *Ensuring that the responsibilities described above will be reassigned if the post holder leaves.*

- [ ] *These tasks will be carried out annually in (you may want to consider using the same date for moving files that you set out in section 4):*

Our archive champions/representatives are (add names and roles):

Approval of KS for the above:

Names, roles and date agreed

Section 6: Further steps

If, once you have established your digital archive, you are looking for ways to build on it, there are a few ways you might want to consider doing this:

Improving records management

As you begin to implement practices to support a digital archive, this should affect the way that you create, store and use files as you work. The best point to start thinking about digital preservation is the point at which the files are created, and many issues with digital archives are caused by a lack of records management procedures. If you have these procedures in place for your paper records, you could look to adapt these for your digital records (e.g. organised filing systems, destruction of files after a certain amount of time).

Improving this could involve:

- Storing files in a more organised manner, which can be moved to the archive with little to no 'tidying'
- Using preservation friendly formats at the point when files are created. The US Library of Congress has a useful recommended formats guide and the DPC's guidance notes and topical notes also cover recommended formats for certain file types. Many of these are widely available/used formats.
- Using file naming conventions, to make sure that file names are useful and show clearly what the file contents are. Using a file naming scheme can also help to normalise the records management and archiving processes in people's ways of working.
- Creating some rules for electronic communications: e.g. ensuring that important decisions aren't only recorded in a WhatsApp group, or by email, but are logged somewhere in your central filing system.
- Creating a 'standard' filing structure for projects or areas of work that are similar, to make these systems easier to navigate and understand across the organisation.

Improving records management involves changing the way people work with their files, and so it can be a slow process, and you may encounter some resistance. It is important to keep emphasising that improving these processes can make filing systems more efficient and therefore make working with them easier.

Allowing access to archives

Archives are meant to be used, and this should be encouraged where possible. There are some things to consider before allowing access to archives:

- Data sensitivity: you may already have closure periods recorded for sensitive personal or medical data, but you should also consider their sensitivity to your organisation's current operations: could this information being open put that in jeopardy, or could it potentially cause harm or distress to someone?
- Practicalities of access: if someone wants to view files in the archives, how will this work: will they be able to access the original files 'in situ', or will you create copies of the files to send to the person requesting them?

At least initially, you should restrict access to the archive to people within your organisation, to use for reflection or 'lesson learning' purposes. Requests from external researchers should be very carefully considered.

List of resources

A list of all resources referred to in each section of this document

Introduction and key concepts

Below are some more detailed definitions of the concepts described in these sections:

International Council on Archives (ICA) What are archives? https://www.ica.org/discover-archives/what-are-archives/

JISC Archives Hub, What are archives? https://archiveshub.jisc.ac.uk/guides/whatarearchives/

Digital Preservation Coalition (DPC) Digital Preservation Topical Note 1: What is Digital Preservation? https://www.dpconline.org/docs/dpc-technology-watch-publications/topical-notes-series/1862-dp-note-1-what-is-digital-preservation/file

MSF CRASH, Historicising Humanitarian Action. Synchronicity in Historical Research and Archiving Humanitarian Missions https://msf-crash.org/en/humanitarian-actors-and-practices/historicising-humanitarian-action-synchronicity-historical

DPC, Digital Preservation Topical Note 4: File Naming and Formats https://www.dpconline.org/docs/dpc-technology-watch-publications/topical-notes-series/1865-dp-note-4-file-naming-and-formats/file

DPC, Digital Preservation Topical Note 5: Metadata https://www.dpconline.org/docs/dpc-technology-watch-publications/topical-notes-series/1866-dp-note-5-metadata/file

Section 1

If you want to create something more formal to present, you could make a business case, which is a more structured request which outlines what you need, and why. The DPC have created a toolkit on how to create a business case for digital preservation here: https://www.dpconline.org/digipres/implement-digipres/business-case-toolkit

The DPC have also produced an Executive Guide on digital preservation which includes some useful arguments to use when advocating for digital preservation: https://www.dpconline.org/digipres/implement-digipres/dpeg-home [also available in French, Spanish and Arabic]

If you want to prepare a short summary of the topic to help you raise awareness with the people you work with, there is a useful guide for creating an elevator pitch here: https://writingcenter.catalyst.harvard.edu/elevator-pitches

For advice on how to talk to IT professionals about digital preservation, see this article: https://minds.wisconsin.edu/handle/1793/78844

NASIG (formerly the North American Serials Interest Group) have produced an introductory guide to digital preservation which includes some good, clear points which may help when starting conversations with stakeholders https://nasig.org/Digital-Preservation-101

Section 2

If you want to do a fuller assessment of your digital material, the DPC have produced a toolkit for creating a digital asset register: https://www.dpconline.org/digipres/implement-digipres/dar-toolkit

If you are interested in managing email archives in more depth, ePADD is a free to download, open source software that helps to appraise, manage and navigate email archives: https://www.epaddproject.org/home

The UK National Archives have also produced some guidance on preserving emails: https://www.nationalarchives.gov.uk/archives-sector/advice-and-guidance/managing-your-collection/preserving-digital-collections/email-preservation-workflows/

If you are considering archiving your social media output, the DPC have an introduction to preserving it here: https://www.dpconline.org/docs/dpc-technology-watch-publications/topical-notes-series/1869-dp-note-9-preserving-social-media/file

If you are considering archiving your website, the DPC have an introduction to web preservation here: https://www.dpconline.org/docs/dpc-technology-watch-publications/topical-notes-series/1861-dp-note-10-preserving-the-web/file

If you are considering archiving your WhatsApp data, in 2018 the DPC published a case study on the capture of WhatsApp records at the United Nations Framework Convention on Climate Change (UNFCCC) which contains some helpful observations: https://www.dpconline.org/blog/wdpd/whatsapp-records-capture

The UK National Archives have produced a framework for records retention for charities. While a lot of the legislation referred to is specific to the UK but it still includes some useful guidance for retention periods with some case studies: https://cdn.nationalarchives.gov.uk/documents/archives/management-framework-for-retention-and-transfer.pdf.

If you store important files in line of business systems (i.e. software and systems that you use for specific purposes, e.g. financial management) the UK National Archives have produced some useful guidance on how to preserve important files created and stored in these systems: https://www.nationalarchives.gov.uk/archives-sector/advice-and-guidance/managing-your-collection/preserving-digital-collections/line-of-business-systems/

Section 3

IThe DPC has a helpful introduction to storage and backup: https://www.dpconline.org/docs/dpc-technology-watch-publications/topical-notes-series/1863-dp-note-2-back-up-and-storage/file

The DPC's preservation system procurement toolkit includes a more detailed checklist for preservation system requirements: https://www.dpconline.org/docs/digital-preservation/procurement-toolkit/2581-core-requirements-for-a-digital-preservation-system-v1/file [also available in Dutch]

Audiovisual Preservation consultants (AVP) have produced a checklist for things to ask about when considering whether cloud storage is suitable for digital preservation: https://www.weareavp.com/nine-things-to-consider-when-assessing-cloud-storage/ [available in Spanish and English]

The InterPARES Trust have also produced a similar checklist for cloud service contracts: http://interparestrust.org/assets/public/dissemination/NA14_20160226_CloudServiceProviderContracts_Checklist_Final.pdf

The Digital POWRR (Preserving digital Objects With Restricted Resources) project has produced a grid showing which digital preservation tools and software do certain activities, which could be useful for choosing a solution(s) which suits you https://digitalpowrr.niu.edu/digital-preservation-101/tool-grid/

Section 4

Steps 1 and 2 (Select and transfer and Ingest) of the UK National Archives Digital preservation workflows contain some useful guidance on transferring digital files to an archive, and some recommendations for tools that can be used if you are interested in building out this process https://www.nationalarchives.gov.uk/archives-sector/advice-and-guidance/managing-your-collection/preserving-digital-collections/digital-preservation-workflows/1-select-and-transfer/

Chapter 5 of Practical Digital Preservation: A How-to Guide for Organizations of Any Size by Adrian Brown includes some useful considerations when preparing for the transfer stage. This book is available from the Internet Archive [requires a free account to log in and borrow the book online]: https://archive.org/details/practicaldigital0000brow/page/108/mode/2up

Section 5

To embed your digital archive into your organisation, it can be very helpful to have a digital preservation policy which outlines what you do, and why. The DPC have produced a toolkit to produce a high level policy: https://www.dpconline.org/digipres/implement-digipres/policy-toolkit

NASIG (formerly The North American Serials Interest Group) have produced a model digital preservation policy. Although this is primarily aimed at organisations who are looking to preserve published digital material, the content and structure could be useful: https://nasig.org/NASIG-model-digital-preservation-policy

If you are planning on using a file profiling tool to assess your file formats, DROID, a free tool created by the UK National Archives is a good starting point. Their website, including download instructions and how to guides, is here: https://www.nationalarchives.gov.uk/information-management/manage-information/preserving-digital-records/droid/

If you would like to find another recommended tool, the International Council on Archives (ICA) have produced a list: https://www.ica.org/ica-network/expert-groups/paag/survival-kit-software/file-format-analysis-tools/

If you are planning on using checksums to check the fixity of your content, there are some useful guides on the methods and tools that you can use for this:

- DPC, DPC Technology Watch Guidance Note: Which checksum algorithm should I use? https://www.dpconline.org/docs/technology-watch-reports/2399-twgn-checksums-addis/file
- National Digital Stewardship Alliance (NDSA) Checking your digital content https://www.digitalpreservation.gov/documents/NDSA-Fixity-Guidance-Report-final100214.pdf

Section 6

If you're thinking more about how you can improve your electronic records management, the UK National Archives have a guide on some basic steps that can be taken to do this: https://cdn.nationalarchives.gov.uk/documents/information-management/managing-electronic-records-without-an-erms-publication-edition.pdf

The World Bank Group have produced a more in depth roadmap which gives a fuller process for improving records management at your organisation: https://www.worldbank.org/en/archive/aboutus/records-management-roadmap [also available in French and Spanish]

UNICEF's Information Management Toolkit also gives a useful guide to the role of information management in emergency work: https://www.ungei.org/sites/default/files/Information-Management-Officer-Role-Humanitarian-Response-2016-eng.pdf

If you're interested in opening up access to your archives, it can help to have a strategy. The DPC have produced a guide for this: https://www.dpconline.org/docs/technology-watch-reports/2495-dpc-guidance-note-developing-an-access-strategy-for-digital-archival-material/file

If you want to improve your digital preservation processes, there are a few tools that you can use to assess your current situation and see where improvements can be made:

- The National Digital Stewardship Alliance's Levels of Digital Preservation model: https://ndsa.org/publications/levels-of-digital-preservation/
- The UK National Archives' DiAGRAM risk assessment tool: https://diagram.nationalarchives.gov.uk/index.html

Other useful toolkits and training

The following toolkits could be useful or interesting to users of this toolkit, and some have also inspired and informed the production of this toolkit.

If you are interested in managing risk to physical archives, UNESECO have produced a toolkit for disaster risk management for archives: https://www.unesco.org/en/articles/building-resilience-disaster-risk-management-documentary-heritage-and-digital-archives-training

The DPC have produced a toolkit for community archives groups to help them preserve digital material, which covers some of the same topics as this toolkit: https://www.dpconline.org/digipres/implement-digipres/community-archives-dp-toolkit

The DPC's Digital Preservation Handbook gives a detailed overview of digital preservation principles and processes. You may want to refer to it as you work through this process
https://www.dpconline.org/handbook [also available in French and Italian]

The DPC and Archives Wales' Digital Preservation for Small Businesses: An Introductory Guide gives a helpful overview of how a small organisation with no previous knowledge can start implementing digital preservation: https://archives.wales/staff-toolkit/records-at-risk/digital-preservation-for-small-businesses-an-introductory-guide/

The Society of American Archivists (SAA) has produced a resource kit for rapidly preserving material produced in response to crises: https://www2.archivists.org/advocacy/documenting-in-times-of-crisis-a-resource-kit

The DPC have also created a free, online training course to introduce people to digital preservation: https://www.dpconline.org/digipres/prof-development/n2kh-online-training. This course offers a good introduction to the key issues and concepts for digital preservation, and takes a few hours to complete.